

# **Securing Unified Communications: From Consumer-Based IM to Enterprise Collaboration and Beyond**

**FaceTime Communications, Inc.**

---

## Table of Contents

<b>Executive Summary</b>	3
<b>The Changing Face of the Web</b>	4
<b>The Business Challenges of Real-time Communications</b>	6
<b>Unified Communications: The Light at the End of the Tunnel?</b>	7
<b>Presence: The New Dial Tone</b>	9
<b>Securing and Managing UC Environments</b>	11
Message hygiene and compliance imperatives for real-time communications	11
Hygiene	11
Compliance	12
The devil is in the details	12
<b>Meeting the Challenge</b>	13
FaceTime Unified Security Gateway	13
Meeting the hygiene requirements	14
Meeting the compliance requirements	14
Delivering security and manageability to the enterprise	15
Flexible deployment	15
A peek under the hood	15
<b>Summary</b>	17
<b>About FaceTime Communications</b>	18
<b>More Information</b>	18

This white paper is for informational purposes only. FaceTime makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of FaceTime Communications, Inc. © 2001 - 2007 FaceTime Communications, Inc. All rights reserved. FaceTime and the FaceTime logo are registered trademarks of FaceTime Communications Inc. FaceTime IMAuditor, RTGuardian, Greynet Enterprise Manager, GEM, RTG and Enterprise Edition are trademarks of FaceTime Communications Inc. All other trademarks are the property of their respective owners.

WP0121-1107 USG

## Executive Summary

---

Internet communications have changed. The user-initiated traffic of real-time communications has created a far more complex environment than simple email exchange and web-browsing - an environment that is dominated by highly evasive greynets such as IM, Skype, P2P and web conferencing. Employees – especially the younger generation – introduce these consumer-grade applications into the corporate environment to gain the same efficiencies of real-time communications in the workplace as they've grown to expect in their personal lives. But these applications circumvent existing security infrastructure, making it difficult for IT administrators to gain visibility and control.

In an attempt to control the situation, many large organizations are deploying unified communications platforms such as Microsoft Office Communication Server and IBM Lotus Sametime. However, the consumer-grade applications and networks are not going away. FaceTime research has found that three out of four employees in organizations where enterprise IM platform has been deployed continue to use public instant messaging systems from providers such as AOL, Yahoo, MSN and Google.

These trends create a heterogeneous network environment that must be secured and managed by IT. Real-time Internet applications pose myriad network and information security risks because they provide vectors for malware, client-side code vulnerabilities, intellectual property loss, and identity theft. Even when an enterprise UC platform is deployed, security and compliance must still be managed from a central point of control, along with enforcement of policies to safely manage the inevitable intermingling of consumer and enterprise-grade applications through federation.

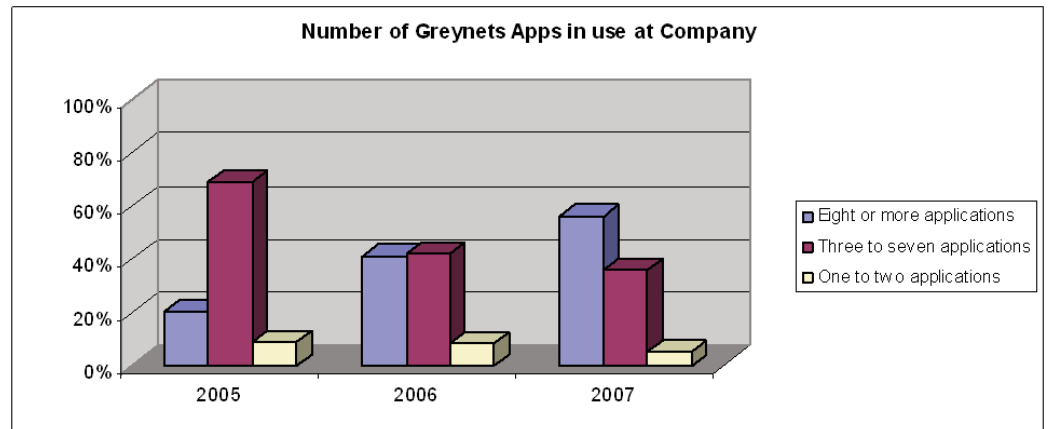
In response to these fundamental changes, FaceTime Communications has introduced the Unified Security Gateway - the first network appliance to leverage presence technology to enable security, management and compliance on a single platform for web and real-time communications traffic in the enterprise. The Unified Security Gateway is a secure Web gateway appliance that enables enterprises to manage real-time Web applications along with consumer-driven unified communication applications such as public IM, Skype and web-conferencing as well as enterprise-class UC platforms such as Microsoft's Office Communications Server and IBM Lotus Sametime.

The Unified Security Gateway combines FaceTime's best in class IM hygiene, IM logging and archiving and gateway malware protection in addition to URL filtering, in a single, purpose-built security and management appliance. Using this single point of control for securing and managing the real-time Internet greatly reduces total cost of ownership, in addition to providing a simpler solution that is more easily updated and maintained by the IT staff.

## The Changing Face of the Web

The first generation of the web was largely a one-way medium - business owners had storefronts, and publishers had publications, but users were not invited to contribute to the process. With the maturation of email as a communications channel and the rapidly-increasing use of real-time communication modalities such as instant messaging, users began to push the web towards a true conversational medium.

The widespread use of greynets - the applications facilitating these real-time, synchronous communications channels - reflects the fast-moving pace of today's personal and working lives. Immediacy is key, and the synchronicity of media like instant messaging, peer-to-peer networks, Voice over IP, web conferencing, social networking, and streaming audio/video is taking over from the older, less-personal, asynchronous approaches of web-browsing and email.



▶  
**Figure 1: The growth trend in greynet application usage is continuing**

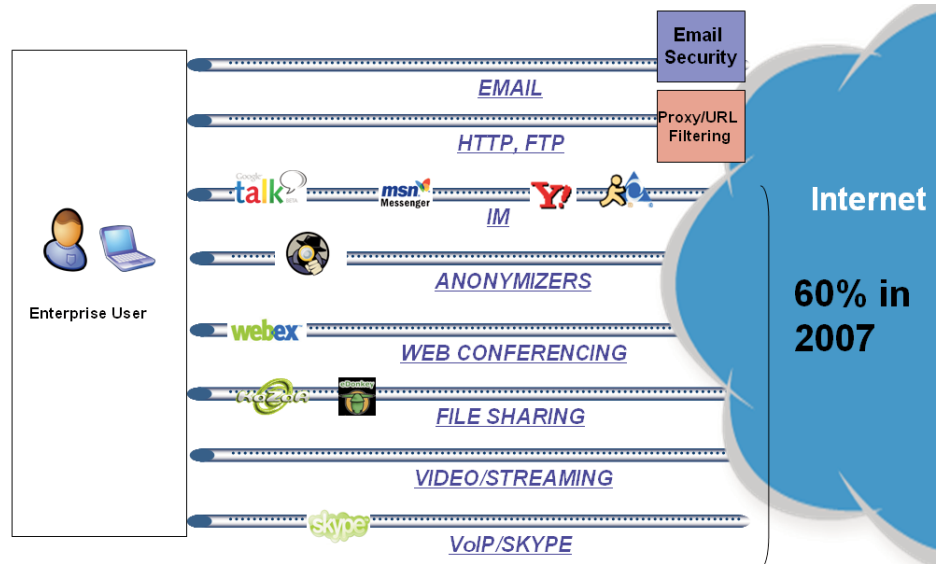
As can be seen in Figure 1 above, the number of greynet applications installed at a typical work location increased significantly between 2006 and 2007, continuing a trend noted in the 2006 survey data. Indeed, the number of work locations with eight or more greynet applications in use has almost tripled in the past three years.

Much of this increase can be attributed to the concurrent growth of telecommuting and emergence of virtual organizations. Research data confirms this:

- 58% of IT executives consider their company to be a virtual workplace
- 75% of IT executives regularly use real-time communications technologies
- 60-70% of employees work in different locations than their managers
- 90% of employees work in locations other than corporate headquarters

This “workplace virtualization” and high degree of decentralization effectively requires real-time communications to ensure efficiency and continuing competitiveness in business, so it’s not surprising that Gartner expects the current 25%-30% adoption level of enterprise instant messaging and unified communications platforms to reach close to 100% by 2010.

▶  
**Figure 2: The majority of communications traffic today is real-time**



Many business are now dealing with half-a-dozen or more disparate real-time communications protocols, all of which IT needs to manage and secure; whether or not these greynet applications are authorized for use on the corporate network, they are using the network to reach out to the wider world through the web gateway.

In addition to fixed (desktop) and semi-mobile (laptop) devices, the wide availability of mobile devices with full keyboards, in conjunction with the continuing increase in IM usage, will lead to explosive growth in wireless IM, according to Osterman Research . Again, this change is being driven by younger workers familiar with SMS and texting, but the need is supported by a large percentage of the organizations surveyed by Osterman, as they grapple with managing the communications needs of an increasingly virtualized and decentralized workforce.

## The Business Challenges of Real-time Communications

The ability of the enterprise to respond quickly is now a key element of competitive strategy and a cornerstone of user productivity. Today's workforce expects instant messaging and other real-time communications tools to be available on their desktops and portable devices at all times, just as the workforce of the 1990s viewed email. The edge of the corporate network is rapidly moving beyond the physical network perimeter to include the broader community of customers and trading partners, and end users are driving the process.

Employees are using greynets, sanctioned or not, and that situation is not going to change any time soon. Regardless of whether an enterprise-grade instant messaging platform such as Microsoft Office Communications Server (OCS) or IBM Lotus Sametime has been deployed, or even if use of a public IM network such as AOL Instant Messenger has been blessed by IT, users are continuing to introduce consumer real-time communications tools into the enterprise. Additional FaceTime research indicates that eight in ten employees in organizations where an enterprise IM platform has been deployed continue to use public IM networks such as MSN, Google, and Yahoo.

Clearly, with this degree of entrenchment of both the applications themselves and users' attitudes towards greynet usage, blocking is no longer an option if the business is to remain competitive and retain key employees. Additionally, for already-overburdened IT departments, this proliferation of communications channels is creating a massive increase in network traffic that must be monitored, managed and secured.

Greynet applications are the new reality for enterprise security and pose a myriad of network and information security risks because they provide vectors for malware, client-side code vulnerabilities, intellectual property loss, and identity theft. While some greynets, especially IM and Skype, deliver real business benefits, they and others such as P2P file sharing can also pose significant security threats to the organization, including:

- Loss of confidential information, intellectual property and privacy issues - greynets open large holes for information leakage
- Compliance risks created by "under the radar" parallel communications networks that expose regulated organizations to legal liabilities and financial penalties
- Increased help desk calls and support costs to clean up spyware infections
- Compromised network security from Trojans, viruses and worms spread through Instant Messaging
- Network bandwidth abuse due to P2P file sharing
- User productivity loss from non-business related IM chatting and video/music file sharing

Attitudinal research by FaceTime Communications has found that

- 83% of end users turn to IM for fast response - more than four in ten believe that email is no longer fast enough to meet their needs
- 70% find IM enhances productivity
- 36% believe they should be allowed to install the applications they believe they need on their work PCs, despite corporate policies to the contrary.

More than half of all users surveyed regularly access social networking sites at work, and 85% use their work PCs for personal tasks - shopping, chatting with friends, downloading files, and general web browsing.

## Unified Communications: The Light at the End of the Tunnel?

The need for time-sensitivity and speed in communications has always been critical to success in business. Business users are setting up virtual conferences, collaborating on projects and documents, augmenting phone conversations with chat threads, and exchanging documents across the Internet. Real-time communications build community and collaboration among different corporate locations, remote employees, telecommuters, supply chains, partners, and customers. They're delivering cost savings, lower telecommunications bills, greater accuracy in written transactions, and increased efficiency through rapid decision-making.

Unified Communications (UC) is the platform, typified by Microsoft Office Communications Server and IBM Lotus Sametime, which gives enterprises a way to start managing this somewhat eclectic mix of tools and protocols. At its fullest extent, UC encompasses every technology that integrates voice with other communications protocols - email, instant messaging, presence, video conferencing, and more.

According to research undertaken by InformationWeek, UC tools are slowly being adopted by businesses, with a quarter of companies going beyond the pilot stage and a further 27% planning to deploy in the next two years. Employee access to UC is projected to reach 35% by 2008.

With the federal government and Homeland Security promoting teleworking programs, the rapid growth of unified communications is likely to continue. According to analyst firm Frost & Sullivan, the number of U.S. teleworkers increased by 150% from 1999 to 2005, a growth rate predicted to continue to increase at a similar pace.

"IT executives don't care how it [unified communications] happens," says the firm. "They just want all their apps to work together, whenever they need them, whatever they are."

IBM's unified communications and collaboration products group has shifted their focus from a single product to a platform. According to the program director: "Some people live in Word, some people live in e-mail, some people live in portals. IBM Lotus Sametime as a platform can accommodate a wider variety of users than a product could. The extensibility of the Lotus Sametime client provides access not just to people, but to information and resources."

A program management architect at Microsoft concurs with the general trend in the direction of enterprise UC platforms. The company is centering much of its UC effort on Microsoft Office Communications Server 2007 and Microsoft Exchange Server 2007, and is also moving into voice over Internet Protocol, or VoIP.

Because it is a natural shift from asynchronous written electronic communications (email) to virtually-synchronous electronic written communications (IM), EIM tends to be the entry point to UC for most corporations. While the upside of widespread EIM adoption - increased productivity, efficiencies, and employee satisfaction - is considerable, there are key areas in which caution is required.

---

While UC platforms deliver a measure of additional security and manageability, those provisions are not always sufficient to meet regulatory compliance, e-Discovery and general “duty of care” corporate governance requirements. Research firm Gartner has identified the following specific requirements that are key to the successful deployment of an enterprise IM solution :

- IM hygiene services
  - o Authentication and authorization services
  - o SpIM protection
  - o Anti-virus and other malware controls, including the prevention of BOTs spreading over IM
- Control of public or other unsanctioned IM services
  - o All manifestations, including tunneled IM services and Skype
- Content leakage controls
- Audit, log, and archival
  - o For e-Discovery legislation
  - o For other regulatory compliance
- Establish corporate-wide effective-use/acceptable-use policies for EIM usage

Additionally, while the use of consumer greynets continues alongside UC deployments, those consumer tools are hitchhiking on corporate network channels, introducing further security concerns because they operate below the radar of existing security measures. These applications use identities that can't be verified, so authentication and content filtering policies can't be applied to any information - conversation or files - traversing that channel. Public IM network connections port-hop for the next available connection, so firewalls can't see what connections are being made, and anti-malware can't check the traffic stream for malicious code. Skype now even has its own development platform, which makes it easier to integrate into business processes, but also increases the potential for accidental or deliberate misuse.

The reality of UC requires a policy framework that creates a single converged identity for every user for all their communications applications, enabling comprehensive management and true presence. According to Frost & Sullivan, "Presence is fundamental to unified communications."

## Presence: The New Dial Tone

Presence - the ability to see who's available through what communications channels at which location at any given time - is the cornerstone of the UC revolution. It brings context to all real-time technologies, beginning with IM and moving out to encompass VoIP, streaming audio and video, web conferencing, and more, on both fixed and mobile platforms.

The move towards presence began in the early days of consumer IM and accelerated rapidly into enterprise IM, where presence servers began to appear, along with Rich Presence Engines (RPEs) that enabled consumer and enterprise IM networks to connect and interact. As the value of presence for enterprises grows, it will become more and more deeply integrated with business processes, leveraging location-based services and mobile devices to become a ubiquitous communications resource.

In today's UC environment, presence is at center stage, providing a status indicator that conveys the ability and willingness of a potential communication partner - for example a user - to communicate with another individual or group. The user's client provides presence information to the UC platform, which is then stored in a "presentity" or personal availability record and made available to others to convey availability for communication. It is analogous to the free/busy signal of the telephone network, but with far greater granularity of information and user control.

The new generation of workers does not see these real-time tools as anything more than just that - tools. The technology is immaterial - it's the availability of the tools that's important. Business is all about connections, and the IM client - public or enterprise - is becoming the launch pad for any kind of meeting or communication.

Presence enables more effective and efficient communication within a business setting, allowing users to instantly see who is available in their corporate network, and giving more flexibility to set up short-term meetings and conference calls using the communications channel that's most convenient or preferable to the parties concerned. The result is precise communication that all but eliminates the inefficiency of phone tag or email messaging. An example of the time-saving aspect of presence information might be a driver with a GPS; he/she can be tracked and sent messages on upcoming traffic patterns that, in return, save time and money. According to IDC surveys, employees "often feel that IM gives their work-days the kind of 'flow' that they feel when sitting directly among their colleagues, being able to ask questions of them, and getting the kind of quick responses that allow them to drive on to the next task."

But whether security measures are keeping up with this communications revolution is a different story. Real-time communications falls outside the scope of existing network and asset management tools; they are linked to the identity of an individual user rather than a device or application. And it is a fundamental truth of the security business that users are the weakest link.

Presence introduces many different types of users into the expanded corporate network. Inside the gateway, the enterprise environment needs to impose a corporate presence standard on the many and varied communications protocols used by partners and customers (as well as friends and family) in the outside world, most of which are consumer-grade networks with rather lower security standards than those required inside the gateway.

UC environments introduce a number of additional challenges for IT security personnel. Mobile users need to be governed by different policies depending on their location, the type of device they are using, who they may be communicating with, by what means, about what

---

topics. Federation brings external connections with partners and affiliates right into the corporate network. Compliance requirements now cover all electronic communications – IM, chat threads, Skype conversations, as well as email – so close attention must be paid to archiving, storage and retrieval as well as the actual content of the conversations. And of course, managing and monitoring all of these aspects must be transparent to users, with zero network latency and scale effectively across multiple locations – a tall order indeed.

## Securing and Managing UC Environments

FaceTime's research into user attitudes to and usage of greynets clearly shows a widespread lack of policy enforcement and control over these communications channels. Not surprisingly, one result is that more than 80% of those users have experienced problems with malware infections and other security issues. Equally unsurprising is IT's top reason for adopting some type of UC strategy: security.

- Communications are evolving in "Internet time" while security infrastructure evolves in "fiscal time."
- Real-time communications tools are being developed by large, profitable, public companies.
- The installed base of UC deployments, especially enterprise IM, is expanding rapidly.
- Public real-time communications networks are interfacing directly with UC infrastructure
- Sanctioned and unsanctioned real-time communications tools must be managed through the same process

While email communications are routinely scanned for malware, real-time applications enable malware to hop from unprotected public networks into the enterprise unseen by traditional security solutions. And not only are more attacks entering the network over real-time channels than email, but the attacks themselves are designed to bypass traditional security measures.

Most enterprises also have in place some form of content filtering or data leak prevention safety net to prevent confidential or privileged information from leaking out through email. But email content filtering systems aren't addressing real-time communications channels.

Compliance regulations - SOX, HIPAA, SEC, eDiscovery requirements, and others - largely apply in the same way to all real-time communications as they do to email. Secure storage, easy retrieval of specific content, audit trails, tampering prevention, context preservation - all the processes that are in place for email must now also be applied to IM exchanges and Skype conversations (both chat and voice threads).

### Message hygiene and compliance imperatives for real-time communications

To meet the needs of today's real-time enterprise, specific messaging hygiene and compliance imperatives apply.

#### Hygiene

To fully secure UC communications, all major communications platforms – public and enterprise, IM and P2P – must be addressed. It's not enough to provide coverage for just "the big four" public networks (Google, AOL, Microsoft, Yahoo); one connection with a network that's not covered effectively negates all the coverage by opening up a new hole in the corporate network.

When communications take place in real time, so do zero-day infections, SpIM outbreaks, and information leakage, so an effective solution must deliver proactive protection against malware infections and detect information leaks before the data leaves the network. Malware protection must be backed by a research team that is focused on these advanced, blended threats that enter the network over real-time channels.

The ability to use existing anti-malware tools and integrate with existing directory structures is needed in order to deliver more efficient detection with minimal latency, enable granular policy application, and provide a faster return on investment.

### **Compliance**

To meet the requirements of e-Discovery and other document-production legislation with any degree of efficiency, organizations must be able to guarantee that all electronic messages – email, IM, chat, etc – are stored in, and easily retrievable from, tamper-proof archives. A security solution that also ensures integration with existing email/WORM storage solutions will clearly enhance this process. Additionally, retrieval and review are simplified significantly if policies can be managed through a rich compliance workflow engine.

Finally, transparency through automated generation of disclaimers in end user communications will assist in educating users when policies are violated.

## **The devil is in the details**

There are multiple reasons for this need for vigilance:

**Introduction of malware** - Real-time channels are increasingly targeted by malware, with blended threats hopping from public to enterprise network.

**Increasingly damaging malware** - Not only are more attacks entering the network over greynets than email, but the attacks themselves are becoming more damaging. Crimeware, rootkits, exploits, and other malware are designed to bypass traditional security measures, and real-time communications channels only make that task easier.

**Spam over IM (SpIM)** - Just as malware is moving to the real-time communications platform to bypass existing security measures, spam is moving beyond the email inbox into the real-time stream, further increasing the risk of accidental malware introduction as well as increasing the traffic load.

**Legislative compliance** - Compliance regulations, including eDiscovery, largely apply to real-time communications conversations and chat threads just as they do to email records. Companies need to be able to “connect the dots” for all types of electronic communications, particularly when the installation spans multiple sites.

**Leakage of intellectual property and other key confidential information** - In the same way that malware can hop across peer-to-peer connections unchallenged, proprietary information can be transferred, redirected, or hijacked both inside and outside the company networks using unmonitored real-time channels.

**Insight and control** - Communications that can't be seen can't be monitored. Unverified identities such as “buddy names” prevent appropriate corporate policies from being applied to greynet communications, and the port-hopping behavior exhibited by these applications renders simple blocking controls unusable.

These threats can be inbound or outbound, and undermine the relationships of trust created by presence - not to mention the tens of thousands of dollars and hundreds of hours of IT resources diverted to cleaning up after a greynet-enabled security breach.

## Meeting the Challenge

The upside to all of this is that presence is aggregated at the gateway, creating a single point at which IT can focus its security efforts - the point where the communication hits the cloud. The presence technology that's at the heart of UC infrastructure must drive the policies that keep these multiple communications channels secure. Presence enables the user to see who's available on which channels; IT must follow that lead and ensure that each of those communications channels is visible, managed, and secured to ensure that the business continues to benefit from the increased productivity and operational agility provided by unified communications.

FaceTime recognizes that real-time communications deliver real business benefits, and that IT needs a way to control, monitor and secure these communications that's efficient, compliant, and makes optimal use of existing investments in security technology. With almost a decade of experience in helping organizations to gain the greatest benefits from real-time communications while effectively controlling their insecurities, the company is ideally positioned to deliver a solution that's precisely focused on the point of greatest risk - the gateway.

## FaceTime Unified Security Gateway

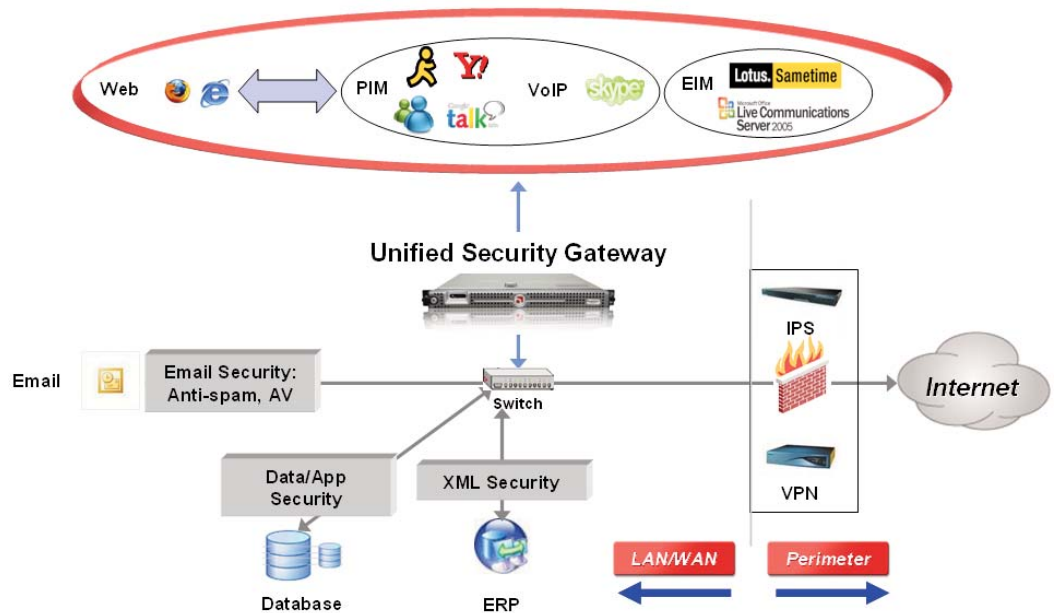
The culmination of FaceTime's deep knowledge and experience in real-time communications, along with the company's close working relationships with Microsoft, IBM Lotus, and other major vendors in the UC marketplace, is the FaceTime Unified Security Gateway (USG)

USG delivers on that knowledge with

- Hardened, proactive security that's built on years of research and partnerships
- TrueCompliance™ to ensure that real-time communications meet and co-exist with current email protection, storage and retrieval standards
- Flexibility and security that enables organizations to evolve UC security as their needs grow and change
- The ability to leverage existing investments in anti-virus and apply those traditional tools to the UC environment

USG enables enterprises to enforce acceptable-use policies for real-time communications and improve visibility into, and decision-making about, security issues related to real-time Internet use. By providing a single point for enablement, access management, security, and control for web and real-time channels, USG delivers a security solution that addresses future as well as current threats while maximizing existing investments in security infrastructure. With flexible deployment options, USG fits seamlessly into existing network topologies to offer the highest level of security with zero latency and a low total cost of ownership.

▶  
**Figure 3: FaceTime USG enables enterprises to optimize their security infrastructure**



FaceTime USG helps organizations meet the requirements identified by Gartner for the effective deployment of a UC environment.

### Meeting the hygiene requirements

USG adds day-zero worm blocking and enhanced SpIM blocking to enterprise instant messaging systems, leveraging existing anti-virus infrastructure to ensure malware-free exchange of information. Real-time content filtering, scanning, and blocking are implemented through global, group, and user-level controls as well as IP-address based controls. USG's ability to recognize and apply policy to the use of dozens of different IM and P2P networks and protocols ensures that all communications sent over unauthorized networks are redirected through an authorized channel such as OCS or SameTime.

### Meeting the compliance requirements

By establishing ethical boundaries and supporting flexible disclaimers to end users, USG ensures that information does not leak inappropriately. Backing this up is a comprehensive archiving of files transferred over IM, Skype, and other chat networks. Rich reporting and workflow includes audit trails.

FaceTime TrueCompliance™ provides strict archiving into email/WORM storage and prevents tampering with granular checksumming of all stored records, also facilitating easy identification and retrieval of specific IM and associated other electronic conversations and communications. Messages can be retained and archived selectively or globally, depending on the organization's message storage locations and the varying demands of different data protection statutes around the world.

---

## Delivering security and manageability to the enterprise

FaceTime's Unified Security Gateway delivers total protection through combined visibility, management and policy control across all unified communications channels. USG empowers enterprises to:

- Get visibility into and control over the use of sanctioned and unsanctioned greynets in the enterprise.
- Enforce security and usage policies across real-time communication and web channels.
- Reduce the business risks from exposure to malware (worms, viruses, SpIM, spyware) and from data leakage.
- Ensure compliance with corporate and regulatory requirements through tamper-proof logging, archival and easy retrieval of electronic conversations.
- Leverage existing security investments by providing an infrastructure that addresses the real-time communications universe.
- Optimize effectiveness with an integrated solution that provides a unified control center for all data channels.

USG combines best-in-class IM management, archival and compliance, perimeter real-time application security, malware prevention, and URL filtering into a single purpose-built hardened Linux appliance. By providing the means for both enablement of productive use of the real-time Internet and the enforcement of policies to manage and monitor for abuse of greynets, FaceTime enables organizations to take control of presence-based channels at the gateway.

### Flexible deployment

USG can be deployed in enablement-only, enforcement-only, or full protection mode.

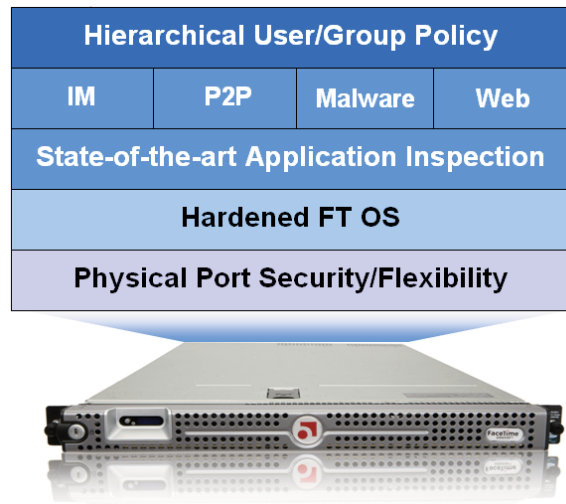
- Enablement-only mode supports four public IM networks (MSN, Yahoo, AOL, Google) and two EIM platforms (Microsoft LCS Connector, Sametime proxy mode). External database support is provided by SQL Server.
- Enforcement-only mode supports 40+ IM networks and 65+ P2P applications. This mode provides gateway malware prevention, URL filtering using SurfControl and Secure Computing databases, and user/group policy enforcement through LDAP integration

Both modes deliver consolidated reporting for all features and multiple-appliance deployments, as well as centralized monitoring.

### A peek under the hood

FaceTime USG architecture is fault-tolerant, avoiding the single-point-of-failure trap and ensuring that, should a server or database go down, messages can still be sent and policies are still applied. The system scales easily to meet enterprise requirements without requiring additional hardware or database servers.

▶ **Figure 4: USG provides both security and enablement in a single device**



At the policy level, USG supports both user and group level policies, inheriting existing policies, and automatically synchronizing them through LDAP integration; it also enforces user authentication using both 'official' user names and 'buddy names'.

At the protocol level, USG delivers finely tuned, granular enforcement of policies relating to greynet applications, enabling or blocking them according to the appropriate policies for different users, situations, and locations. Both signature and behavior-based malware detection strategies are supported, delivering day-zero protection as well as SpIM blocking. Content filtering policies are applied universally, regardless of whether traffic is in the clear (as is usually the case with consumer-level IM) or encrypted (as is the case with Skype chat).

The appliance's centralized OS enables IT to lock down services as required and is hardened against common scripting attacks. SSH access, dedicated management and proxy port services, and both two- and three-port installation options provide for delivery of a single security and compliance solution that addresses all real-time communications channels without impacting their productive use.

## Summary

---

The Internet has changed and is now dominated by real-time communications traffic rather than just email and Web browsing. Enterprises are adopting Unified Communications platforms at a rapid pace, starting with Enterprise IM, in response to the need to optimize workplace productivity and apply some degree of control to the use of consumer-driven technologies, which continue to be used alongside EIM applications. The result is a heterogeneous environment that IT must control and bring into compliance with corporate and government regulatory policies.

FaceTime has developed the Unified Security Gateway (USG) as a single point of enforcement and enablement to allow IT to both control and facilitate the productive use of real-time communications. Traditional e-mail and web content filtering controls are unable to fully address the security and management vulnerabilities introduced by the real-time Internet alone; FaceTime has the expertise to provide for its safe and productive use by leveraging existing investments for the new layers of protection required.

## About FaceTime Communications

---

FaceTime Communications enables the safe and productive use of the real-time Internet, including both public and enterprise instant messaging and unified communications platforms. Ranked number one by IDC in market share among instant messaging management vendors for the fourth consecutive year, FaceTime's award-winning solutions are used by more than 900 customers including nine of the ten largest U.S. banks. FaceTime supports or has strategic partnerships with all leading public and enterprise IM network providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM, Reuters, and Jabber.

### More Information

For more information about FaceTime Communications and FaceTime solutions please visit

<http://www.facetime.com>

FaceTime Communications

1301 Shoreway Rd

Belmont, CA 94002

Phone: (650) 631-6300

Email: [info@facetime.com](mailto:info@facetime.com)